

GEMMA Gegevenslandschap

Logging van verwerking van
(persoons)gegevens

Leeswijzer

Dit document beschrijft de visie van VNG Realisatie ten aanzien van de opslag en ontsluiting van de metagegevens van verwerkingen van objectgegevens. Primair ligt hierbij de focus op de vastlegging van de verwerking van persoonsgegevens. Dit document behoort tot de architectuurdOCUMENTEN van de ontwikkeling van de gemeentelijke informatievoorziening: het GEMMA Gegevenslandschap. In deze visie worden de gemeentelijke bewegingen op het gebied van de informatievoorziening geschetst, en wordt aan de hand van deze bewegingen een nieuwe, flexibele en meer generieke en gezamenlijke gemeentelijke informatievoorziening geschetst.

Dit document is bestemd voor informatiemanagers, adviseurs, architecten en productmanagers van gemeenten en gemeentelijke leveranciers.

Het document is als volgt opgebouwd:

- Hoofdstuk 1 beschrijft de inleiding;
- Hoofdstuk 2 beschrijft het vigerende beleid en kaders;
- Hoofdstuk 3 beschrijft de huidige- en toekomstige gemeentelijke informatiearchitectuur;
- Hoofdstuk 4 beschrijft de scope van logging van verwerkingen en eisen die eraan gesteld worden;
- Hoofdstuk 5 beschrijft de mogelijke inrichtingsvarianten voor de opslag van de logging;
- Hoofdstuk 6 beschrijft een aantal interactiepatronen;
- Hoofdstuk 7 beschrijft het GEMMA component.

Dit document is in beheer bij VNG-Realisatie.

Versie	Toelichting	Datum	Opsteller(s)
1.0	Eerste vastgestelde versie	November 2018	VNG Realisatie
1.1	Aanpassingen n.a.v. consultatie met gemeenten en leveranciers	Oktober 2019	VNG Realisatie
1.2	Aanpassingen n.a.v. nadere uitwerking API-standaard voor logging van verwerkingen	Maart 2021	VNG Realisatie
1.3	Figuur 12 aangepast n.a.v. nieuw opgenomen applicatiefunctie	April 2021	VNG Realisatie

Inhoudsopgave

Leeswijzer	2
Inhoudsopgave.....	3
1. Inleiding.....	5
2. Beleid en kaders.....	6
2.1. Visie Nederlands kabinet	6
2.2. Europees Kader: Algemene Verordening Gegevensbescherming (AVG).....	7
2.2.1. Rechtmatige verwerking (verwerkingsgrondslag en doelbinding)	7
2.2.2. Dataminimalisatie	7
2.2.3. Juistheid van persoonsgegevens	8
2.2.4. Opslagbeperking (bewaartermijnen)	8
2.2.5. Beveiliging van persoonsgegevens	8
2.2.6. Specifieke aanvullende verplichtingen uit de AVG	9
2.3. Nationaal kader: Uitvoeringswet AVG (UAVG)	11
2.3.1. Regeling van het BSN in de Uitvoeringswet AVG	11
3. Informatiearchitectuur.....	13
3.1. Huidige inrichting	13
3.2. Toekomstige inrichting.....	14
3.3. Uitgangspunten voor huidige en toekomstige situatie.....	16
3.4. Het verwerkingenlog in de informatiearchitectuur	17
4. Scope van, en eisen aan logging van verwerkingen	18
4.1. Scope	18
4.2. Eisen aan logging	18
5. Inrichtingsvarianten	20
5.1. Centrale versus gefedereerde inrichting	21
5.2. Centraal Verwerkingenlog.....	21
5.3. Federatief Verwerkingenlog	23
5.4. Samenvoegen Verwerkingenlogs	24
6. Interactiepatronen	26
6.1. Inzage in het Verwerkingenlog.....	26
6.2. Brongegevens raadplegen.....	27

6.3. Gegevens aanbieden aan externen	29
6.4. Gegevens afnemen bij externen	30
7. GEMMA componenten	32
7.1. Verwerkingenloggingcomponent.....	32
Bijlage 1: Bronnen	34

1. Inleiding

Een van de belangrijke doelen van het kabinet is het versterken van de weerbaarheid van burgers en organisaties. In onder andere de visie Nederland Digitaal en de Digitale Agenda Overheid is verwoord op welke manier hieraan invulling wordt gegeven. Een belangrijk begrip hierbij is verantwoording naar de burger kunnen afleggen over welke persoonsgegevens, voor welk doel en door wie zijn verwerkt. Dergelijke transparantie vergroot het inzicht van de burger en daarmee het vertrouwen van de burger in de overheid.

“Om het vertrouwen in systemen te vergroten, hebben mensen het recht op inzicht wie, op welk moment en voor welk doel, hun gegevens inziet, gebruikt of aan anderen geeft. Dit recht is vastgelegd in de Algemene Verordening Gegevensbescherming. Dit vraagt veel van alle overheidsorganisaties en mogelijk leidt dit tot gezamenlijke acties.”

Bron: NL DIGIbeter - Agenda Digitale Overheid, juli 2018

Het bieden van transparantie naar burgers over de verwerking van (persoons)gegevens heeft gevolgen voor de inrichting van de informatiesystemen van gemeenten. Verwerkingen van (persoons)gegevens, zowel binnen de gemeente als met keten- en netwerkpartijen, moeten vastgelegd worden en deze verwerkingen moeten aan de burger inzichtelijk gemaakt kunnen worden. De huidige gemeentelijke informatiesystemen kunnen maar zeer beperkt voldoen aan deze eisen. Om te borgen dat in de (nabije) toekomst gemeenten invulling kunnen geven aan de gestelde eisen is het van belang om de vastlegging en ontsluiting van verwerkingen (logging) te standaardiseren.

In deze notitie wordt beschreven op welke wijze gemeenten verwerkingen van (persoons)gegevens kunnen vastleggen in logbestanden. Tevens wordt beschreven hoe vanuit deze logbestanden transparantie aan de burger en bestuur geboden kan worden ten aanzien van de verwerking van deze gegevens.

Daar waar in deze notitie wordt gesproken over de gemeente mag ook worden gelezen ‘gemeentelijk samenwerkingsverband’, Regionale Uitvoeringsdiensten of ‘SaaS dienstverlener’ voor een gemeente.

2. Beleid en kaders

2.1. Visie Nederlands kabinet

Digitalisering transformeert wereldwijd economieën en maatschappijen in een razendsnel tempo. Nederland heeft een goede uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. De digitale infrastructuur is van wereldklasse, de beroepsbevolking is goed opgeleid en we hebben een traditie van samenwerking, bijvoorbeeld tussen bedrijfsleven, kennisinstellingen en overheid. Tegelijkertijd roept digitalisering ook nieuwe, fundamentele vragen op. Bijvoorbeeld over de bescherming van onze privacy en de toekomst van onze banen. Om de kansen van digitalisering te benutten en antwoorden te geven op deze vragen moet Nederland vooroplopen met digitalisering. Met onderzoek, experimenten, het toepassen van nieuwe technologie en constructieve discussies over ethische vraagstukken. Op die manier versterken we het Nederlands verdienvermogen, kunnen we beter richting geven aan technologische ontwikkelingen en zetten we vol in op de economische en maatschappelijke kansen van digitalisering. Om voorop te kunnen lopen moeten we ook het vertrouwen van burgers en bedrijven vergroten. Daarom versterken we het fundament – o.a. privacybescherming, cybersecurity, digitale vaardigheden en eerlijke concurrentie – voor digitalisering. De uitdaging bij deze transformatie is om iedereen binnen boord te krijgen én te houden. Op de arbeidsmarkt, maar ook in de samenleving als geheel.

Het kabinet zet daarom in op een aanpak met twee sporen:

1. Maatschappelijke en economische kansen benutten (versnellen)
Digitalisering vindt voor een belangrijk deel plaats in maatschappelijke sectoren waar de overheid een relatief grote rol heeft. Denk aan de zorg, mobiliteit, energie en het agrifood-domein. Ook de verdere digitalisering van het openbaar bestuur zelf is een belangrijke opgave. De uitdaging voor het kabinet is om in deze sectoren de digitale transitie te versnellen en te ondersteunen.
2. Het fundament voor digitalisering – waaronder privacybescherming, cybersecurity, digitale vaardigheden en eerlijke concurrentie – moet op orde zijn en verder worden versterkt. Het kabinet zet hiervoor in op vijf speerpunten, zodat burgers en bedrijven de kansen kunnen benutten die digitalisering biedt.

Het fundament van Nederland Digitaal is nader uitgewerkt in 'NL DIGIbeter 2020', de Agenda Digitale Overheid van alle overheden gezamenlijk, die in 2020 is vastgesteld door de Ministerraad. Deze agenda legt verbinding met publieke en private partners om kansen en vraagstukken van de digitalisering door de overheid op te pakken. Door NL DIGIbeter 2020 heen staan de behoeften en rechten van burgers en ondernemers centraal. De Agenda biedt enerzijds ruimte om op een innovatieve manier te werken aan maatschappelijke vraagstukken. Aan de andere kant wordt voortgebouwd op de bestaande voorzieningen om de dienstverlening beter en persoonlijker te maken. Bijvoorbeeld door modernisering van de overheidsportalen zodat mensen op één plek zaken met de overheid kunnen regelen die aan hun persoon gekoppeld is.

Verder besteedt de Agenda veel aandacht aan zowel grondrechten en publieke waarden (bijvoorbeeld bij datagebruik) als ook de toegankelijkheid/begrijpelijkheid van digitale dienstverlening (inclusie). Dat betekent dat mensen het recht hebben op digitale dienstverlening, maar ook dat voor inwoners die niet digitaal geholpen kunnen of willen worden er andere vormen van contact mogelijk is.

VNG Realisatie

Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

Belangrijk onderdeel van NL DIGIbeter 2020 is het persoonlijker maken van de dienstverlening, bijvoorbeeld door de inwoner meer inzage en regie te geven op de eigen gegevens. Gemeenten spelen dan ook een grote rol bij de sturing op voorzieningen van de digitale basisinfrastructuur die juist betrekking hebben op die dienstverlening. Denk hierbij aan mijnOverheid en identiteitsmiddelen.

2.2. Europees Kader: Algemene Verordening Gegevensbescherming (AVG)

De AVG is sinds 25 mei 2018 rechtstreeks van toepassing. Met de Uitvoeringswet Algemene verordening gegevensbescherming (zie voor een toelichting hierna) is de Wet bescherming persoonsgegevens (Wbp) ingetrokken. De AVG hanteert voor de bescherming van persoonsgegevens een bepaalde systematiek om op basis van een aantal privacy beginselen te komen tot afgewogen keuzes voor de bescherming van persoonsgegevens. Daarnaast schrijft de AVG aanvullend op een aantal aspecten meer in detail voor hoe persoonsgegevens moeten worden beschermd. In dit kader zijn het meest van belang de “transparantierechten” die aan betrokken worden toegekend en de verplichtingen om privacy by design als uitgangspunt te nemen en een PIA uit te voeren om zicht te krijgen op feitelijk spelende privacy risico's en daarop maatregelen te treffen. De kern van de AVG wordt gevormd door een aantal grondslagen en beginselen dat als uitgangspunt moet worden genomen bij de (inrichting van) verwerking van persoonsgegevens. Deze grondslagen en beginselen worden hieronder toegelicht.

2.2.1. Rechtmatige verwerking (verwerkingsgrondslag en doelbinding)

Uit de AVG volgt in de eerste plaats dat de verzameling en verwerking van persoonsgegevens plaatsvindt op een rechtmatige en behoorlijke wijze (artikel 5, eerste lid, aanhef en onder a, van de AVG). Verder dienen de doeleinden waarvoor verzameling en verwerking plaatsvindt gerechtvaardigd, welbepaald en uitdrukkelijk omschreven te zijn (doelbinding). Voor overheidsorganisaties geldt daarbij dat zij voor de verwerking van persoonsgegevens voor de hen toegekende taken het kader van die taken over een expliciete verwerkingsgrondslag moeten beschikken.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Bij de vastlegging van verwerkingen dienen de doeleinden en verwerkingsgrondslagen waarvoor verzameling en verwerking plaats hebben gevonden te worden geregistreerd zodat verantwoording, zowel naar de burger als naar het bestuur, afgelegd kan worden over de rechtmatigheid van de verwerkingen.

2.2.2. Dataminimalisatie

Persoonsgegevens die worden verwerkt moeten toereikend en ter zake dienend zijn, en beperkt zijn tot wat noodzakelijk is voor de doeleinden. Daarbij gaat het om proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, eerste lid, onder c, van de AVG). Er mogen niet meer gegevens dan nodig worden verwerkt en er moet goed worden gezien of het doel niet op een manier kan worden bereikt die minder inbreuk maakt op privacy.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Bij de vastlegging van verwerkingen dient vastgelegd te worden welke gegevens, of categorieën van gegevens tijdens de verwerking zijn gebruikt. Door deze vastlegging kan verantwoording worden afgelegd over proportionaliteit en subsidiariteit van het verwerkende proces. Bij de vastlegging van de verwerking worden geen inhoudelijke gegevens opgeslagen buiten een identificerend attribuut waarmee de verwerking aan een

persoon of ander object kan worden gerelateerd. Deze vastlegging is nodig om bij een verzoek om inzage de verwerkingen te kunnen koppelen aan de juiste persoon.

2.2.3. Juistheid van persoonsgegevens

De AVG bepaalt ook dat moet worden voorzien in maatregelen om te zorgen dat persoonsgegevens op een juiste wijze worden verwerkt en dat maatregelen worden getroffen om te zorgen dat gegevens die niet (meer) juist worden verwerkt, gerectificeerd of verwijderd worden (artikel 5, eerste lid, onder d, van de AVG).

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Voor wat betreft de vastlegging van verwerkingen heeft deze eis geen directe doorwerking. Het is de verantwoordelijkheid van de processen die gegevens verwerken om invulling te geven aan maatregelen die de juistheid van gegevens borgen.

2.2.4. Opslagbeperking (bewaartermijnen)

Een volgend belangrijk uitgangspunt is dat persoonsgegevens niet langer worden verwerkt dan voor een termijn die geleet op het doel van verwerkingen noodzakelijk en daarmee te rechtvaardigen is (artikel 5 eerste lid, onder f, van de AVG).

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het moet mogelijk zijn om gegevens van verwerkingen te verwijderen die niet langer bewaard hoeven te worden. De bewaartermijn van gegevens is afhankelijk van de verwerkende processen. Bij de vastlegging van de verwerkingen moet aangegeven worden wat de bewaartermijn vanuit het verwerkende proces is zodat de termijn ook gehanteerd kan worden voor de vastgelegde gegevens over de verwerkingen (de logging).

2.2.5. Beveiliging van persoonsgegevens

Bij de verwerking van persoonsgegevens moeten technische en organisatorische maatregelen worden getroffen, zodanig dat een passende beveiliging gewaarborgd is (artikel 5, eerste lid, onder f, van de AVG). Ten aanzien van de beveiliging van persoonsgegevens werkt artikel 32 van de AVG dit uit. Bepaald wordt dat, waar passend, pseudonimisering en versleuteling ingezet moet worden. NB: pseudonimisering is dus niet per definitie verplicht, maar kan als oplossing behulpzaam zijn bij problemen ten aanzien van herleidbaarheid en het voorkomen van kwetsbare gegevensconcentraties. Ook wordt aangegeven dat maatregelen moeten worden genomen om te zorgen dat op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen kan worden gegarandeerd, en dat de beveiligingsmaatregelen op gezette tijden getest en geëvalueerd worden. Voorts volgt uit dit artikel dat dient te worden voorzien in maatregelen om, bij een fysiek of technisch incident, de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te kunnen herstellen. Voor de inrichting van beveiliging van persoonsgegevens dient rekening te worden gehouden met de zogeheten Richtsnoeren beveiliging Persoonsgegevens, waarin de AP de wijze waarop beveiliging van persoonsgegevens kan plaatsvinden nader heeft uitgewerkt¹.

¹ <http://wetten.overheid.nl/BWBR0033572/2013-03-01>

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Aan burgers moet inzage gegevens kunnen worden in de persoonsgegevens die door de gemeente verwerkt zijn. Om deze transparantie te kunnen bieden is het vereist om de vastgelegde verwerkingen te kunnen koppelen aan de burger. Voorkomen moet worden dat de vastlegging van verwerkingen leidt tot een kwetsbare gegevensconcentratie. Denk bijvoorbeeld aan het vastleggen van een onversleutelde BSN in de logging. Dit zou kunnen leiden tot een privacy hotspot doordat verwerkingen over verschillende organisaties en processen via het BSN aan elkaar gekoppeld kunnen worden. Uitgangspunt is daarom dat dergelijke gegevens gepseudonimiseerd worden alvorens de verwerking wordt vastgelegd in de logging.

2.2.6. Specifieke aanvullende verplichtingen uit de AVG

Naast de modellering van bescherming van persoonsgegevens aan de hand van deze beginselen, regelt de AVG ter ondersteuning en kadering daarvan ook nog een aantal meer concrete verplichtingen. De in dit kader meest relevante verplichtingen worden hieronder besproken.

Inregelen faciliteiten voor uitoefening rechten betrokkenen

Transparantie voor betrokkenen heeft in de AVG een belangrijke plaats gekregen. Een van de kernprincipes in de AVG is dat burgers zicht en controle kunnen houden over hun persoonsgegevens en kunnen ingrijpen als dat nodig is (hoofdstuk 3 AVG). De AVG kent aan burgers rechten tot om controle te houden over hun gegevens. Veel rechten zoals het inzage- en correctierecht, golden al onder de Wbp, maar een aantal rechten is nieuw of meer in de aandacht gezet, zoals het "vergeetrecht (op verzoek wissen van gegevens)" en het recht op overdraagbaarheid van gegevens ("dataportabiliteit").

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het vergeetrecht is ten aanzien van de vastgelegde verwerkingen beperkt van toepassing. In de logging worden naast een gepseudonimiseerde identiteit geen persoonsgegevens vastgelegd. Het recht op dataportabiliteit is niet van toepassing aangezien het gaat om de vastlegging van daadwerkelijk uitgevoerde verwerkingen door een specifieke organisatie. Dergelijke gegevens zijn niet overdraagbaar naar een andere organisatie.

Privacy by design (& by default)

De AVG verplicht expliciet om in het ontwerp (design) van systemen en standaardinstellingen (default) reeds van het begin af aan rekening te houden met bescherming van persoonsgegevens. Er dienen bij het ontwerp zowel technische als organisatorische maatregelen te zijn getroffen die de gegevensverwerking strikt beperken tot de noodzaak en persoonsgegevens mogen in beginsel – systeemtechnisch, d.w.z. zonder bewuste keuze - niet verwerkt/gedeeld worden.

Privacy by design komt er kortgezegd op neer dat bij de inrichting en inregeling van systemen en processen die de noodzakelijke verwerkingen van persoonsgegevens ondersteunen rekening wordt gehouden met de bescherming van persoonsgegevens. In feite betreft dat een weerslag van afweging tussen de genoemde privacy beginselen een invulling van de wijze waarop aan transparantieplichtingen kan worden voldaan.

Privacy by default komt erop neer dat bij oplevering van een nieuwe voorziening standaard alles dicht staat en voor het openstellen van bijv. toegang expliciet actie nodig is.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Door geen inhoudelijke (persoons)gegevens vast te leggen maar alleen meta-gegevens over een verwerking wordt de gegevensverwerking beperkt tot de strikt noodzakelijke gegevens. Als technische maatregel wordt pseudonimisering toegepast om te voorkomen dat identificerende gegevens van burgers misbruikt kunnen worden.

Data protection impact assessment (DPIA)

Uiteindelijk gaat het bij de bescherming van persoonsgegevens om het voorkomen van privacy risico's en (vooral ook) om het voorkomen van onwenselijke gevolgen ervan voor burgers.

Naar aanleiding van de motie-Franken heeft het kabinet bepaald dat bij de ontwikkeling van beleid en wetgeving waaruit gegevensverwerkingen voortvloeien, bij de bouw van ICT-systemen en de aanleg van grote databestanden een DPIA moet worden uitgevoerd. De AVG verplicht tot het voorafgaand uitvoeren van een DPIA voor gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van natuurlijke personen. Daarvan wordt in elk geval geacht sprake te zijn als er sprake is van verwerkingen van persoonsgegevens met een hoog risico, zoals bij de inzet van nieuwe technieken of grootschalige gegevensverwerking - voorafgaand daarop – een DPIA uit te voeren. Doel er van is om – aanvullend op de inrichting van bescherming van persoonsgegevens op grond van de reeds besproken beginselen, scherper zicht te krijgen op de feitelijk bij de verwerking of in de context spelende privacy risico's en daarmee – als correctiemechanisme - rekening te houden bij de uiteindelijke (ontwerp) en beveiligingsmaatregelen.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het uitvoeren van een DPIA op een voorgestelde inrichting van de vastlegging van logging van de gemeentelijke informatiesystemen lijkt gezien de verwerking van het BSN in de logging noodzakelijk te zijn².

Sluitstuk AVG: register- en verantwoordingsplicht

De AVG vereist dat organisaties (zowel verantwoordelijken als verwerkers) aantoonbare controle hebben over de persoonsgegevens die zij verwerken. Dit betekent dat een register moet worden bijhouden van alle verwerkingen van persoonsgegevens die plaatsvinden. De AVG schrijft concreet voor welke gegevens ten aanzien van verwerkingen moeten worden bijgehouden. Ook moet actief aandacht worden besteed aan, en maatregelen geïmplementeerd waaruit blijkt dat de organisatie de AVG-beginselen voor verwerking van persoonsgegevens naleeft.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Gemeenten zijn verplicht een register van verwerkingen te voeren. Informatiesystemen die een verwerking van persoonsgegevens uitvoeren dienen deze verwerking te relateren aan een doelbinding en grondslag uit het

² Zie: <https://www.informatiebeveiligingsdienst.nl/nieuws/checklist-data-privacy-impact-analyse/>

gemeentelijk register. In de vastlegging van de verwerking van gegevens door gemeentelijke informatiesystemen worden de doelbinding en grondslag als meta-gegevens bij de verwerking vastgelegd.

2.3. Nationaal kader: Uitvoeringswet AVG (UAVG)

Met de UAVG wordt uitvoering gegeven aan de AVG. De AVG is een Europese verordening. Dat betekent dat voor de lidstaten nog maar beperkt ruimte is voor de nationale wetgever om op het terrein van de verwerking van persoonsgegevens zelf iets (afwijkends) te regelen. Daar waar de verordening nog wel ruimte laat voor nationale keuzes, is gekozen om zo dicht mogelijk te blijven bij de Wbp (beleid-neutrale implementatie). In dit verband is het meest relevant dat artikel 87 van de AVG een grondslag geeft om bij nationaal recht specifieke voorwaarden te stellen voor de verwerking van nationale identificatienummers, in Nederland onder meer het BSN.

2.3.1. Regeling van het BSN in de Uitvoeringswet AVG

De Uitvoeringswet AVG regelt het gebruik van wettelijk voorgeschreven nummers, beleidsneutraal en overeenkomend met het voorheen geldende artikel 24 van de Wbp. De nu geldende regels voor verwerking van het BSN worden dus gecontinueerd. Dit betekent dat voor verwerking van het BSN een wettelijke grondslag nodig is. Voor overheidsorganen betreft artikel 10 van de Wabb. Voor de verwerking van het BSN door private partijen betekent de regeling dat dient te worden voorzien in een specifieke wettelijke grondslag. Hieronder wordt dit nader toegelicht.

Artikel 46 van de UAVG regelt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. In feite is dit een kapstokbepaling, op basis waarvan in andere wetten invulling kan worden gegeven aan dergelijke nummers.

In de praktijk bestaat soms de wens het BSN ook voor andere doelen te gebruiken dan ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. Dit is alleen gerechtvaardigd als aan twee vereisten is voldaan. Ten eerste geldt het algemene vereiste dat persoonsgegevens alleen verder mogen worden verwerkt als dat verenigbaar is met de doeleinden waarvoor ze zijn verkregen. Ten tweede bepaalt artikel 46 van de Uitvoeringswet dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Dit is een aanvullende eis op die van verenigbaarheid omdat het gebruik van persoonsnummers extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, zoals bijvoorbeeld identiteitsfraude.

Eventuele andere gebruiksdoelen dienen derhalve door de formele wetgever zelf te worden vastgesteld. Er komt ten aanzien van de verdere verwerking van het BSN geen eigen afweging toe aan de verwerkingsverantwoordelijke. Hiermee is in de Uitvoeringswet gebruik gemaakt van de nationale ruimte die de verordening biedt om specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer op grond van artikel 6, tweede lid, en 87 van de verordening.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het BSN mag door gemeenten worden gebruikt als dat noodzakelijk is voor de goede vervulling van hun publiekrechtelijke taak. De Wet algemene bepalingen burgerservicenummer (Wabb) biedt deze wettelijke grondslag voor gemeenten. Bij het loggen van verwerkingen van die vanuit de publieke taak worden uitgevoerd is het derhalve toegestaan om het BSN, het liefst gepseudonimiseerd, op te slaan. Voor de

privaatrechtelijke taken van een gemeente ligt dat anders³. Voor het gebruik van het BSN in dat kader is geen wettelijke grondslag. Het gebruik van het BSN is binnen de processen van de bedrijfsvoering derhalve niet rechtmatig.

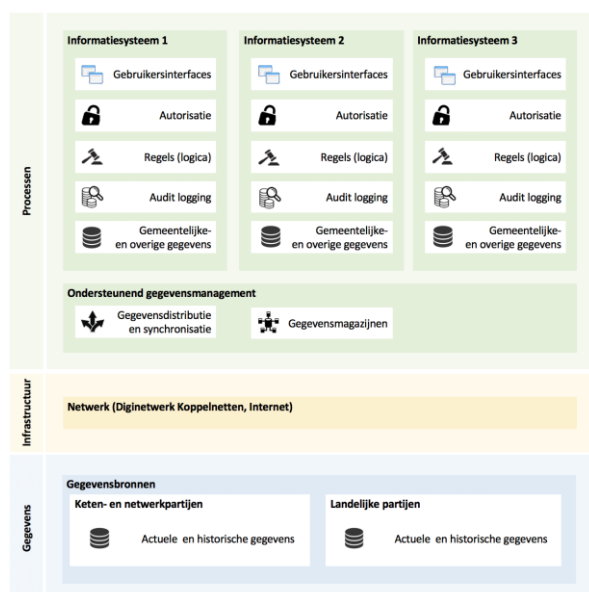
De verplichting om de burger inzage te geven in de verwerking van persoonsgegevens geldt voor zowel publiek- als privaatrechtelijke verwerkingen. Bij het loggen van verwerkingen die voortvloeien uit de privaatrechtelijke taken van een gemeente dient een ander identificerend attribuut gebruikt te worden dan het BSN.

³ <https://autoriteitpersoonsgegevens.nl/nl/nieuws/gebruik-bsn-de-bedrijfsvoering-van-de-overheid>

3. Informatiearchitectuur

3.1. Huidige inrichting

Gemeenten maken voor de uitvoering van hun taken gebruik van een groot aantal gegevensverwerkende informatiesystemen. Deze informatiesystemen zijn veelal gericht op de ondersteuning van een specifiek gemeentelijk domein. Voorbeelden van dergelijke domeinen zijn sociale zaken, belastingen en burgerzaken. Daarnaast wordt door gemeenten gebruik gemaakt van informatiesystemen die een meer horizontale taak hebben. Voorbeelden hiervan zijn documentsystemen en gegevensmagazijnen. Al deze informatiesystemen worden zowel qua functionaliteit als gebruikte gegevens door leveranciers afgebakend. Daar waar mogelijk wordt door leveranciers gebruik gemaakt van nationale- en internationale standaarden, bijvoorbeeld op het gebied van gegevensmodellering (denk aan het Suwi-Gegevensregister⁴ en INSPIRE⁵).



Figuur 1 Gemeentelijke informatiesilo's

De gemeentelijk informatiesystemen bieden zelfstandig gebruikersinterfaces, autorisatie, bedrijfsregels, logging en gegevensopslag en werken hierdoor feite als informatiesilo's. Gegevens die door deze silo's

⁴ <https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr>

⁵ <https://www.geonovum.nl/onderwerpen/inspire>

worden verwerkt uit basisregistraties worden via binnengemeentelijke synchronisatie- en distributiemechanismen synchroon gehouden met de basisregistraties.

In de huidige situatie gebruiken gemeenten informatiesystemen van (veel) verschillende leveranciers die elk op hun eigen manier de gegevensverwerking vormgeven. Dit levert voor gemeenten een ingewikkelde informatievoorziening op waarin het voldoen aan de eisen uit informatiebeveiliging- en privacy wet- en regelgeving een complexe uitdaging is. Informatiesystemen zijn meestal niet ingericht op de eisen die vanuit de AVG gesteld worden. Principes zoals het kennen en vastleggen van een 'doelbinding' als grond voor een verwerking van persoonsgegevens worden binnengemeentelijk slechts in uitzonderingsgevallen geïmplementeerd. Het is hierdoor voor gemeenten in de praktijk bijna onmogelijk om de verwerking van persoonsgegevens in- en extern op een adequate manier te verantwoorden. De opzet en complexiteit van het gemeentelijk applicatielandschap biedt ook niet de verwachting dat op korte termijn volledig aan de eisen vanuit de AVG voldaan kan worden.

3.2. Toekomstige inrichting

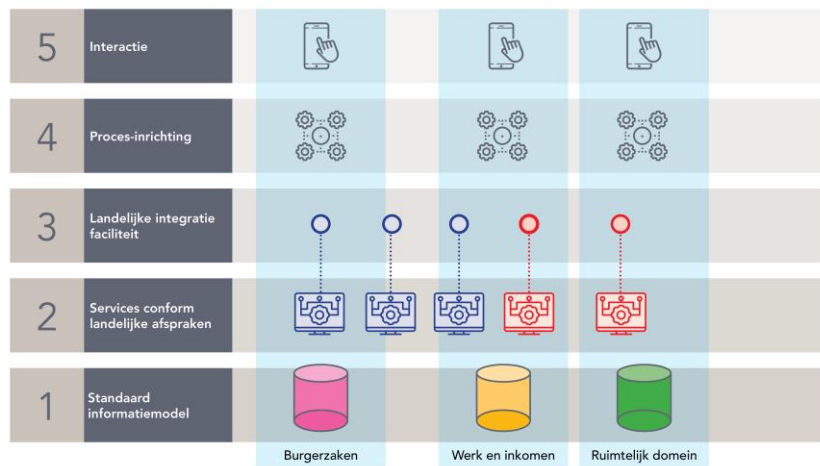
Gemeenten moeten groeien naar een situatie waarin burgers eenvoudig kunnen worden gefaciliteerd in hun AVG-rechten. Gemeenten moeten op een laagdrempelige en inclusieve manier aan burgers inzage kunnen geven welke medewerker, op welk moment welke persoonsgegevens voor welk doel heeft verwerkt. In de huidige informatievoorziening is het lastig om hier invulling aan te geven doordat systemen hierop niet zijn ingericht.

Door gemeenten is daarom een nieuwe inrichting van de gemeentelijke informatievoorziening geschetst in de 'Informatiekundige visie Common Ground'⁶. Kern van deze visie is het scheiden van processen en gegevens en het bevragen van gegevens bij de bron. Onderdeel van de informatiekundige visie is een vijf-lagenmodel waarmee verantwoordelijkheden van informatiesystemen logisch, en ook fysiek van elkaar gescheiden kunnen worden in:

- Interactie met eindgebruikers,
- Inrichting van processen,
- Integratiefunctie
- Ontsluiting van gegevens via gestandaardiseerde diensten, en
- Gestandaardiseerde modellering van gegevens.

Het grote voordeel van de inrichting van informatiesystemen volgens dit model is dat het meer ruimte biedt om sneller en gemakkelijker te innoveren. Het Common Ground model maakt gemeenten minder afhankelijk van hun vaste leveranciers en geeft burgers en ondernemers meer en beter inzicht in de wijze waarop met hun gegevens wordt omgegaan.

⁶ <https://vng.nl/samen-organiseren/common-ground>



Figuur 2 Common Ground vijf-lagen model

Door VNG Realisatie is het Common Ground vijf-lagenmodel nader uitgewerkt naar functionaliteiten die door de verschillende lagen moeten, of kunnen, worden geboden. Deze nadere uitwerking, ook wel *het GEMMA Gegevenslandschap*⁷ genoemd, schetst de informatiearchitectuur voor de informatiesystemen en gegevensbronnen van de toekomst.

Uitgangspunt binnen het gemeentelijk gegevenslandschap is dat alle verwerkingen van gegevens worden uitgevoerd conform vastgestelde doelbinding en grondslagen, en worden gelogd voor verantwoordingsdoeleinden. Onderdeel van het gemeentelijk gegevenslandschap is een register van verwerkingsactiviteiten waarin wordt bijgehouden welke verwerkingen van persoonsgegevens plaatsvinden binnen de gemeenten en met welke wettelijke grondslag dit gebeurt. Vanuit het GEMMA Gegevenslandschap wordt aan informatiesystemen de verplichting opgelegd dat verwerkingen van persoonsgegevens altijd gerelateerd zijn aan een in het register van verwerkingsactiviteiten opgenomen verwerkingsactiviteit. Daarnaast wordt de verplichting opgelegd om verwerkingen van persoonsgegevens vast te leggen in een verwerkingenlog en de relevante onderdelen van deze verwerkingenlog open te stellen naar burgers.

Informatiesystemen die volgens de uitgangspunten van het GEMMA Gegevenslandschap worden ontwikkeld kunnen hierdoor voldoen aan de Verantwoordingsplicht⁸ zoals opgenomen in de AVG.

⁷ <https://www.gemmaonline.nl/index.php/Gegevenslandschap>

⁸ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht>

3.3. Uitgangspunten voor huidige en toekomstige situatie

De huidige gemeentelijke informatiesystemen voldoen slechts in zeer beperkte mate aan de eisen die vanuit de AVG-verantwoordingsplicht worden gesteld. Deze informatiesystemen moeten hierop aangepast worden. Tegelijkertijd worden nieuwe gemeentelijke informatiesystemen ontwikkeld waarin processen en gegevens van elkaar gescheiden zijn en verantwoording van verwerking van persoonsgegevens vanuit het ontwerp van het systeem zijn meegenomen (privacy by design). Gemeenten zullen de komende jaren een mix van informatiesystemen gebruiken die in meer of mindere mate ontworpen zijn vanuit beginselen van de bescherming van de privacy. Toch moeten gemeenten voldoen aan de eisen die vanuit de AVG op het gebied van de Verantwoordingsplicht zijn vastgesteld door de wetgever. Ook de huidige gemeentelijke informatiesystemen zullen invulling moeten gaan geven aan de eisen die vanuit de Verantwoordingsplicht worden gesteld.

Ten aanzien van invulling van de Verantwoordingsplicht moet de gemeente invulling geven aan de volgende uitgangspunten:

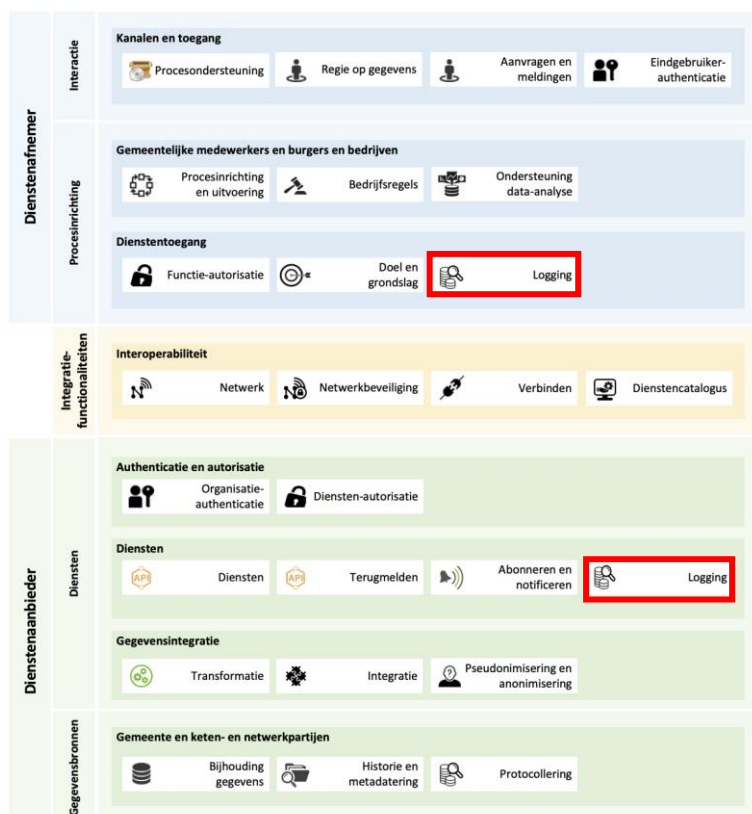
- De gemeente voert een register van verwerkingsactiviteiten waarin wordt vastgelegd welke (persoons)gegevens door de gemeente worden verwerkt, met welke doelbinding en welke grondslag;
- Verwerkingen van persoonsgegevens worden gerelateerd aan een verwerkingsactiviteit (de combinatie van een doelbinding en een grondslag) uit het register van verwerkingsactiviteiten;
- De metagegevens van een verwerking van persoonsgegevens worden vastlegt in een verwerkingenlog;
- Het verwerkingenlog dient als bron voor de duiding van de verwerking van persoonsgegevens door de gemeente richting burger en bestuur;
- Gegevens uit het verwerkingenlog moeten voor een bepaalde tijd verborgen kunnen worden voor burgers om te voorkomen dat de burger voortijdig op de hoogte wordt gebracht van bijvoorbeeld onderzoeken in het kader van fraudebestrijding;
- Voor het vastleggen van de verwerking van persoonsgegevens wordt gebruik gemaakt van de API-standaard die hiervoor beschikbaar is⁹.

De bovenstaande uitgangspunten doen recht aan de binnen wet- en regelgeving gestelde eisen en gelden voor alle informatiesystemen die (persoons)gegevens verwerken, zowel informatiesystemen die op de huidige- als de nieuwe inrichtingsprincipes zijn gebaseerd. Door in de manier van het loggen van verwerkingen en het hanteren van doelbinding en grondslagen geen onderscheid te maken in informatiesystemen die gebaseerd zijn op de 'oude' of 'nieuwe' inrichtingsprincipes wordt het voor gemeenten mogelijk om voor de verantwoording van verwerkingen van persoonsgegevens gebruik te maken van één verwerkingenlog, ongeacht het type informatiesysteem.

⁹ <https://github.com/VNG-Realisatie/gemma-verwerkingenlogging>

3.4. Het verwerkingenlog in de informatiearchitectuur

Door VNG Realisatie is de gewenste informatiearchitectuur beschreven in het ‘GEMMA Gegevenslandschap’¹⁰. Onderdeel van het gemeentelijk gegevenslandschap is, conform vereisten vanuit de AVG, de vastlegging van de verwerking van persoonsgegevens. Vanuit het GEMMA Gegevenslandschap wordt aan informatiesystemen de verplichting opgelegd via de daartoe vastgestelde standaard¹¹ verwerkingen van persoonsgegevens vast te leggen in een verwerkingenlog. Ook wordt de verplichting opgelegd om dit verwerkingenlog open te stellen naar geautoriseerde afnemers.



Figuur 3 GEMMA Gegevenslandschap

In bovenstaand figuur is weergegeven dat het onderdeel “Logging” zich zowel bevindt in de procesinrichtinglaag van dienstenafnemers als in de dienstenlaag van dienstenaanbieders. Hiermee wordt duidelijk gemaakt dat het de verantwoordelijkheid van de zowel de afnemer als de leverancier van een dienst is om de verwerking van persoonsgegevens in een verwerkingenlog vast te leggen.

¹⁰ https://www.gemmaonline.nl/index.php/Thema_Samen_organiseren

¹¹ <https://github.com/VNG-Realisatie/gemma-verwerkingenlogging>

4. Scope van, en eisen aan logging van verwerkingen

4.1. Scope

In de “*Aanwijzing logging*”¹² van de Informatiebeveiligingsdienst (IBD) worden verschillende vormen van logging uitgebreid beschreven. De scope van dit document beperkt zich uitsluitend tot logging die betrekking heeft op de vastlegging van de verwerking¹³ van persoonsgegevens. Doel van deze logging is het duiden van verwerkingen die zijn uitgevoerd op persoonsgegevens. De logging is niet bedoeld voor het maken van reconstructies van situaties en gegevens in systemen op een bepaald tijdstip in het verleden. Voor verwerkingen van persoonsgegevens is vastlegging van de verwerking verplicht, voor de verwerking van overige objecten is deze optioneel.

4.2. Eisen aan logging

Aan de gegevens die ten aanzien van verwerkingen worden vastgelegd worden een aantal eisen gesteld. Deze eisen liggen op het gebied van de vertrouwelijkheid, integriteit, actualiteit, volledigheid en rechtmatigheid.

Actualiteit

Het is de verantwoordelijkheid van zowel een dienstenaanbieder als een dienstafnemer om te borgen dat verwerkingen van persoonsgegevens worden vastgelegd in het verwerkingenlog. Indien een verwerking niet kan worden vastgelegd dan mag de verwerking ook niet worden uitgevoerd.

¹² <https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

¹³ EU-AVG, Art.4: "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Volledigheid

Het is de verantwoordelijkheid van zowel een dienstenaanbieder als een dienstenafnemer om bij de uitvoering van een proces de verwerking van alle betrokken personen vast te leggen. Het is mogelijk dat binnen een proces de gegevens van meerdere personen worden verwerkt. Denk hierbij bijvoorbeeld aan een dienst die op basis van een zoekopdracht gegevens van meerdere objecten (bv personen) terug geeft. Om te borgen dat per object inzicht kan worden gegeven in de verwerkingen moet voor ieder object waarvan gegevens worden verwerkt apart de verwerking vastgelegd worden.

Bij de uitvoering van de publieke taak worden door gemeenten (persoons)gegevens uitgewisseld met keten- en netwerkpartijen. Bij het verwerken van deze gegevens moet door beide partijen de verwerking in een eigen verwerkingenlog worden vastgelegd.

Integriteit

De logregistratie dient als bron voor de verantwoording van de rechtmatigheid van verwerkingen door de gemeente. De inhoud van de logregistratie dient boven alle twijfel verheven te zijn. Logbestanden dienen derhalve immutable (onaanpasbaar) te zijn. Op geen enkele wijze mag het mogelijk zijn om de logbestanden aan te passen worden na het aanmaken van een logrecord zonder dat dit zichtbaar is. Een eventuele correctie dient in de vorm van een nieuw record te worden toegevoegd zodat eenmaal aangemaakt records nooit gewijzigd worden. Zowel technische als organisatorische maatregelen moeten getroffen worden om dit te borgen.

Privacy

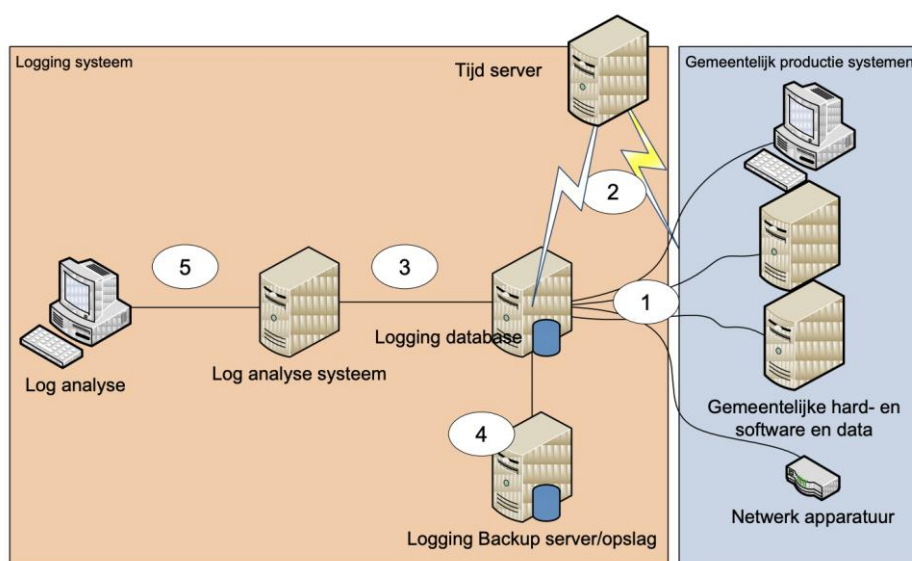
Er moet worden voorkomen dat het verwerkingenlog privacy risico's introduceert. Voorkomen moet worden dat het verwerkingenlog een privacy hotspot kan worden van waaruit een profiel van een burger opgesteld kan worden. Eventuele identificerende eigenschappen van persoonsgegevens dienen gepseudonimiseerd te worden alvorens in het verwerkingenlog opgenomen te worden. Het gebruik van pseudoniemen voorkomt dat de gegevens uit het verwerkingenlog direct kan worden gerelateerd aan een persoon.

Rechtmatigheid

Het verwerkingenlog wordt door de gemeente gebruikt om zowel naar burgers als bestuur de verwerking van persoonsgegevens mee te verantwoorden. Om aan te tonen dat een verwerking rechtmatig is geweest is het van belang dat bekend is wie de verwerking heeft uitgevoerd en vanuit welke doelbinding en grondslag deze persoon de verwerking heeft uitgevoerd. Al de informatie die vereist is voor het kunnen afleggen van verantwoording en het bieden van transparantie dienen in het verwerkingenlog opgenomen te worden.

5. Inrichtingsvarianten

Informatiesystemen die (persoons)gegevens verwerken dienen metagegevens ten aanzien van deze verwerkingen vast te leggen in een verwerkingenlog. Onderstaand figuur geeft weer hoe een logging opzet er globaal uit ziet.



Figuur 4 Globale inrichting logging¹⁴

Logging wordt vanuit de systemen naar een centrale logging database gezonden.

1. Alle systemen hebben dezelfde tijd en gebruiken een tijd synchronisatie bron.
2. De logging database wordt benaderd vanuit een loganalyse systeem.
3. Logging die langere tijd ongebruikt blijft wordt apart gezet in een back-up server.
4. Het loganalyse systeem wordt gebruikt door loganalyse werkstations.

¹⁴ Bron: Logging aanwijzing gemeentelijke informatiebeveiligingsdienst.
<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

5.1. Centrale versus gefedereerde inrichting

Ten aanzien van zowel het gemeentelijk register van verwerkingsactiviteiten (VAR) als het verwerkingenlog (VWL) geldt dat deze componenten éénmaal (centraal) of meerdere malen (gefedereerd) in de gemeentelijke informatievoorziening kunnen worden geïmplementeerd. Beide scenario's kennen voor- en nadelen.

Vanuit het oogpunt van beheersbaarheid wordt aanbevolen om het VAR als centrale component te implementeren. In dit centrale scenario worden alle verwerkingsactiviteiten van de verschillende gemeentelijke domeinen ondergebracht in één gemeentelijk register van verwerkingsactiviteiten. Door een centrale inrichting te kiezen is het voor de FG eenvoudig om overzicht te houden over de door de organisatie gehanteerde verwerkingsactiviteiten en kunnen koppelingen met andere systemen zoals een ISMS¹⁵ eenvoudiger worden gerealiseerd.

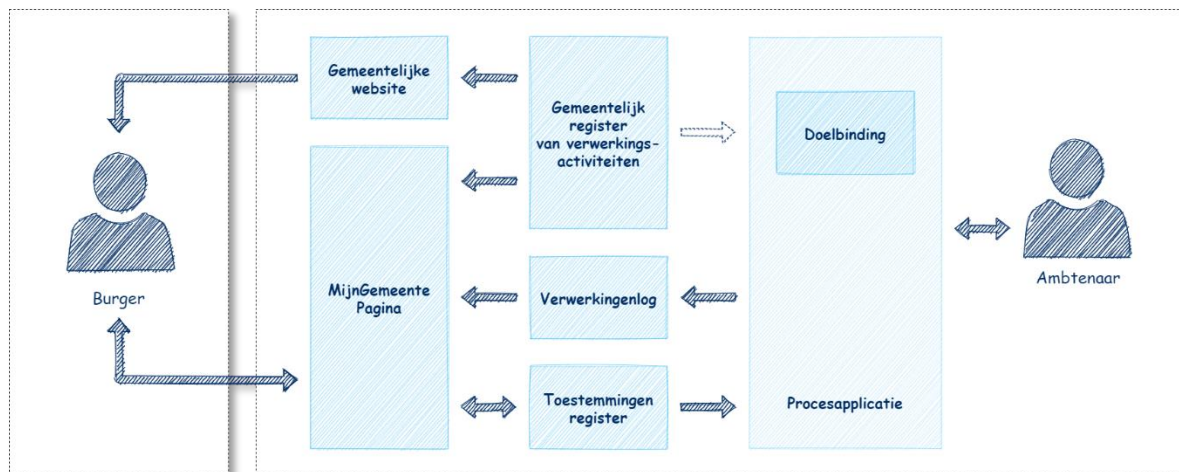
Wat voor het VAR geldt, geldt ook voor het verwerkingenlog. Gemeenten kunnen ervoor kiezen om een centraal VWL binnen de gemeente in te richten of te kiezen voor een inrichting waarbij per domein of procesapplicatie een VWL wordt bijgehouden.

Beide inrichtingen kennen voor- en nadelen. Voordeel van een centrale inrichting is dat vanuit een centrale bron alle verwerkingenlog gegevens ontsloten kunnen worden naar burgers en geautoriseerde gemeentelijke medewerkers. Nadeel van deze inrichting is dat er een potentiële privacy hotspot ontstaat aangezien alle verwerkingen rondom personen in één bron worden bijgehouden. Door analyse van de patronen van verwerkingen rondom een persoon is het in bepaalde situaties mogelijk om gevoelige gegevens af te leiden.

5.2. Centraal Verwerkingenlog

Onderstaande afbeelding schetst een samenhang van de componenten die in algemene zin voorkomen bij het loggen van verwerkingsactiviteiten bij een implementatie met een centraal Verwerkingenlog.

¹⁵ Informatiesysteem voor een procesgerichte benadering voor informatiebeveiliging. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd. Bron: <https://www.informatiebeveiligingsdienst.nl/product/isms-v1-0/>



Figuur 5 Centraal Verwerkingenlog

Een burger kan via de Gemeentelijke website het openbare gedeelte van het Gemeentelijk register van verwerkingsactiviteiten raadplegen. Dit register bevat genoeg algemene informatie voor de burger om te kunnen inzien voor welke verwerkingsactiviteiten de gemeente persoonsgegevens verwerkt.

In het centraal Gemeentelijk register van verwerkingsactiviteiten zijn alle verwerkingsactiviteiten opgenomen die door de gemeente kunnen worden uitgevoerd. Een Procesapplicatie voert maar een aantal verwerkingsactiviteiten uit het gehele register uit. Het ligt daarom voor de hand dat elke Procesapplicatie alleen de UUID's van die verwerkingsactiviteiten uit het centrale register overneemt die van belang zijn. Elke applicatiefunctie in de Procesapplicatie die een persoonsgegevensverwerking uitvoert, wordt gekoppeld aan zo'n verwerkingsactiviteit en vastgelegd als Doelbinding in de Procesapplicatie. Dit gebeurt tijdens de configuratie of inrichting van een (nieuwe) Procesapplicatie of als er wijzigingen zijn doorgevoerd in het VAR die van belang zijn voor de Procesapplicatie.

De Procesapplicatie legt de logging van de verwerkingsactiviteit die is uitgevoerd op persoonsgegevens vast in het centraal VWL. Een burger kan via het centraal VWL inzien welke verwerkingen door de gemeenten voor de uitvoering van de publieke taak zijn uitgevoerd op zijn of haar persoonsgegevens. Omdat het VWL alleen de unieke nummers van de verwerkingsactiviteiten bevat, worden de loggegevens eerst nog gecombineerd worden met de gegevens uit het VAR zodat een begrijpelijk en samenhangend resultaat aan de burger kan worden getoond. Bij de verwerkingen wordt het BSN van de betreffende burger vastgelegd. Omdat de gegevens in het VWL privacygevoelig zijn, zijn ze pas in te zien nadat de burger via een beveiligd portaal (MijnGemeente Pagina) is aangemeld. De aanmelding gebeurt via een door de Wet digitale overheid (Wdo) goedgekeurd authenticatiemiddel (bijvoorbeeld DigiD) op minstens betrouwbaarheidsniveau Substantieel. De medewerker die de verwerkingsactiviteiten via de Procesapplicatie uitvoert, heeft geen inzage in het Verwerkingenlog, niet via de Procesapplicatie en niet rechtstreeks. Dit is door middel van autorisatie afgeschermd.

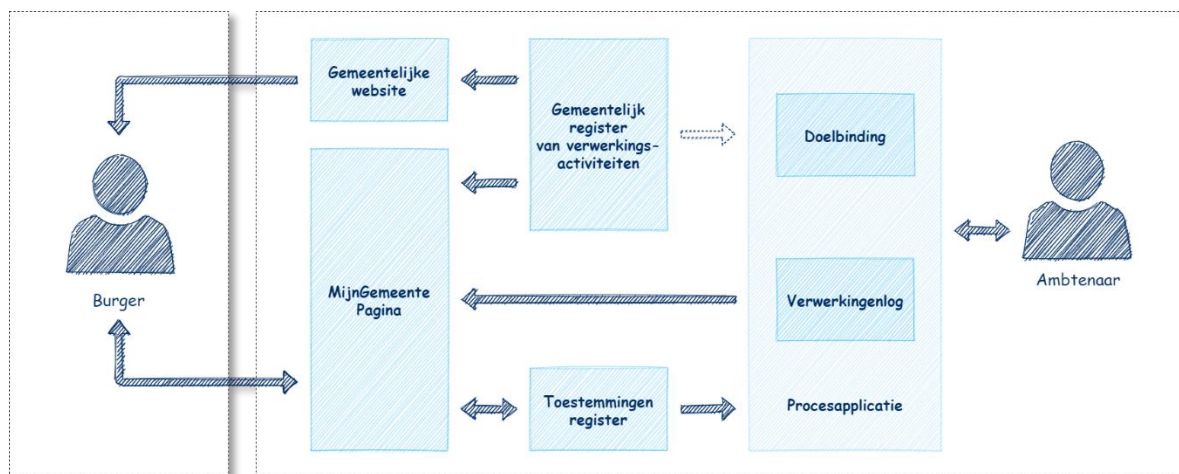
Via de MijnGemeente Pagina kan de burger ook zijn toestemmingen op het gebruik van de persoonsgegevens vastleggen. Dit Toestemmingregister wordt door een Procesapplicatie geraadpleegd om te controleren of een burger toestemming heeft verleend voor een verwerkingsactiviteit. De verwerkingsactiviteit wordt vervolgens uitgevoerd met als grondslag van de verwerkingsactiviteit 'Toestemming van de burger'. Het Toestemmingenregister valt buiten de scope van de uitwerkingen in dit document.

VNG Realisatie

Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

5.3. Federatief Verwerkingenlog

Onderstaande afbeelding schetst een samenhang van de componenten die in algemene zin voorkomen bij het loggen van verwerkingsactiviteiten bij een implementatie met een federatief Verwerkingenlog.



Figuur 6 Federatief Verwerkingenlog

Een burger kan via de Gemeentelijke website het openbare gedeelte van het Gemeentelijk register van verwerkingsactiviteiten raadplegen. Dit register bevat genoeg algemene informatie voor de burger om te kunnen inzien voor welke verwerkingsactiviteiten de gemeente persoonsgegevens verwerkt.

In het centraal Gemeentelijk register van verwerkingsactiviteiten zijn alle verwerkingsactiviteiten opgenomen die door de gemeente kunnen worden uitgevoerd. Een Procesapplicatie voert maar een aantal verwerkingsactiviteiten uit het gehele register uit. Het ligt daarom voor de hand dat elke Procesapplicatie alleen de UUID's van die verwerkingsactiviteiten uit het centrale register overneemt die van belang zijn. Elke applicatiefunctie in de Procesapplicatie dat een persoonsgegevensverwerking uitvoert, wordt gekoppeld aan zo'n verwerkingsactiviteit en vastgelegd als Doelbinding in de Procesapplicatie. Dit gebeurt tijdens de configuratie of inrichting van een (nieuwe) Procesapplicatie of als er wijzigingen zijn doorgevoerd in het VAR die van belang zijn voor de Procesapplicatie.

Een leverancier van een Procesapplicatie kan ervoor kiezen het Verwerkingenlog in de Procesapplicatie in te bouwen, een zogenoemd federatief VWL. Het federatief VWL moet dan wel van buiten de Procesapplicatie te benaderen zijn. Een extra variant is dat een andere Procesapplicatie ook gebruik maakt van de ingebouwde VWL om de logging vast te leggen.

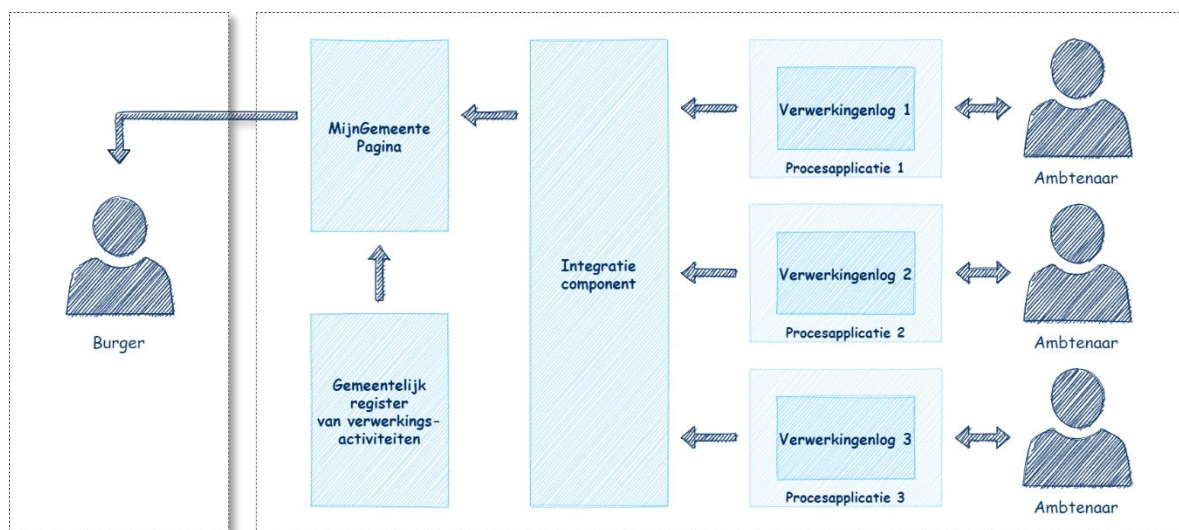
De Procesapplicatie legt de logging van de verwerkingsactiviteit die is uitgevoerd op persoonsgegevens vast in het federatief VWL. Een burger kan via het federatief VWL inzien welke verwerkingen door de gemeenten voor de uitvoering van de publieke taak zijn uitgevoerd op zijn of haar persoonsgegevens. Omdat het VWL alleen de unieke nummers van de verwerkingsactiviteiten bevat, worden de loggegevens eerst nog gecombineerd worden met de gegevens uit het VAR zodat een begrijpelijk en samenhangend resultaat aan de burger kan worden getoond. Bij de verwerkingen wordt het BSN van de betreffende burger vastgelegd. Omdat de gegevens in het VWL privacygevoelig zijn, zijn ze pas in te zien nadat de burger via een beveiligd portaal

(MijnGemeente Pagina) is aangemeld. De aanmelding gebeurt via een door de Wet digitale overheid (Wdo) goedgekeurd authenticatiemiddel (bijvoorbeeld DigiD) op minstens betrouwbaarheidsniveau Substantieel. De medewerker die de verwerkingsactiviteiten via de Procesapplicatie uitvoert, heeft geen inzage in het Verwerkingenlog, ook niet via de Procesapplicatie. Dit is door middel van autorisatie afgeschermd.

Via de MijnGemeente Pagina kan de burger ook zijn toestemmingen op het gebruik van de persoonsgegevens vastleggen. Dit Toestemmingregister wordt door een Procesapplicatie geraadpleegd om te controleren of een burger toestemming heeft verleend voor een verwerkingsactiviteit. De verwerkingsactiviteit wordt vervolgens uitgevoerd met als grondslag van de verwerkingsactiviteit 'Toestemming van de burger'. Het Toestemmingenregister valt buiten de scope van de uitwerkingen in dit document.

5.4. Samenvoegen Verwerkingenlogs

Een gemeente gebruikt meerdere Procesapplicaties waarin persoonsgegevens worden verwerkt. De federatieve Verwerkingenlogs worden door een centraal component bevraagd dat de loggegevens samenvoegt tot één gegevensset en dit doorgeeft aan de MijnGemeente Pagina.



Figuur 7 Samenvoegen verwerkingenlogs

Als een burger een aanvraag doet voor inzage in de verwerkingsactiviteiten van zijn of haar persoonsgegevens, moeten alle federatieve Verwerkingenlogs waarover een gemeente beschikt, geraadpleegd worden. De MijnGemeente Pagina moet dan elk federatief Verwerkingenlog apart bevragen, combineren met gegevens uit het Gemeentelijk register van verwerkingsactiviteiten en vervolgens samenvoegen tot een logisch geheel voor de burger.

Om te voorkomen dat de MijnGemeente Pagina bij elk federatief VWL gegevens moet ophalen, wordt een apart integratiecomponent hiervoor gepositioneerd. Dit integratiecomponent wordt dan door de MijnGemeente Pagina bevraagd en het resultaat wordt aan de burger getoond. Vaak wordt voor deze integratiefunctie een (Enterprise) Service Bus (ESB) ingezet. In dit component wordt geconfigureerd hoe en in welke volgorde

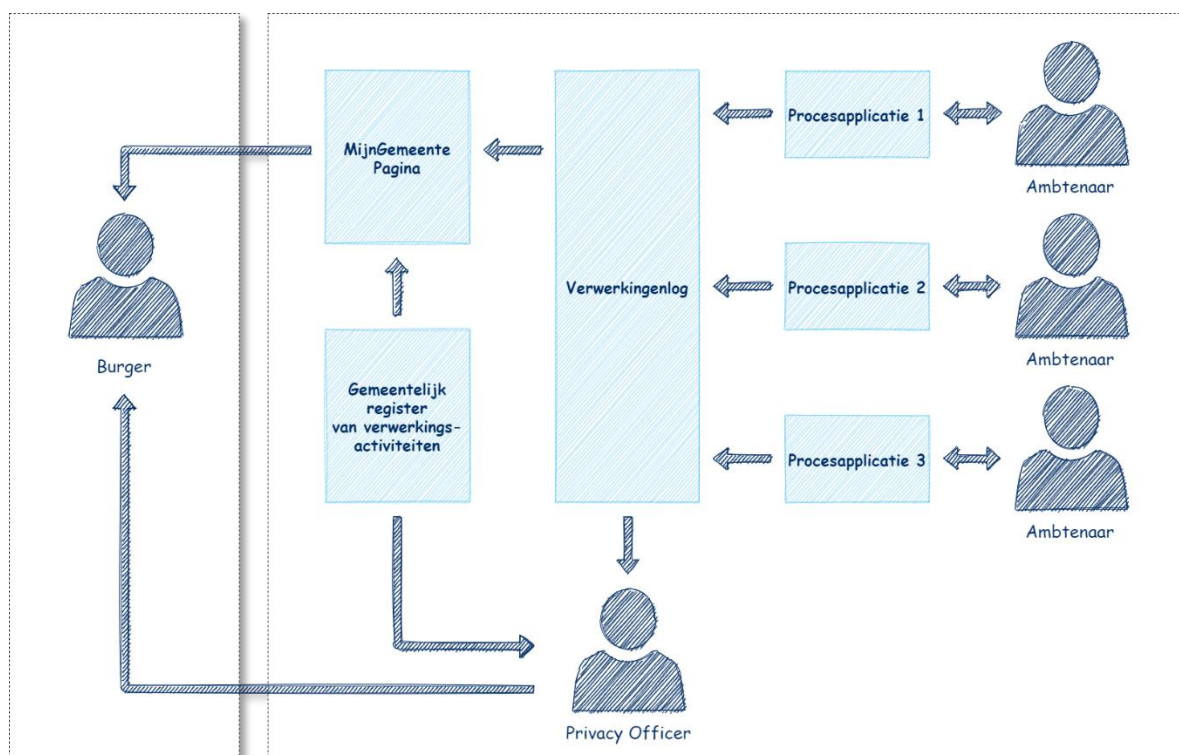
alle federatieve Verwerkingenlogs bevraagd worden. Omdat het VWL alleen de unieke nummers van de verwerkingsactiviteiten bevat, moeten de loggegevens daarna nog gecombineerd worden met de gegevens uit het VAR en als één geïntegreerd resultaat worden weergegeven. Als er nieuwe registers beschikbaar komen, kunnen de verwijzingen naar die registers op één centrale plek binnen de ESB eenvoudig worden toegevoegd.

De medewerkers die de verwerkingsactiviteiten via de Procesapplicaties uitvoeren, hebben geen inzage in de Verwerkingenlogs, niet via de Procesapplicatie en niet rechtstreeks. Dit is door middel van autorisatie afgeschermd.

6. Interactiepatronen

6.1. Inzage in het Verwerkenlog

Onderstaande schets geeft een beeld hoe de inzage van een Verwerkenlog door een bevoegde medewerker van een gemeente kan worden vormgegeven. In onderstaand voorbeeld is de bevoegde medewerker een Privacy Officer.



Figuur 8 Inzage in verwerkenlog

Elke Procesapplicatie registreert de verwerkingsactiviteiten in het Verwerkenlog. De medewerker die de verwerkingsactiviteiten via de Procesapplicatie uitvoert, heeft geen inzage in het Verwerkenlog, niet via de Procesapplicatie en niet rechtstreeks. Dit is door middel van autorisatie afgeschermd.

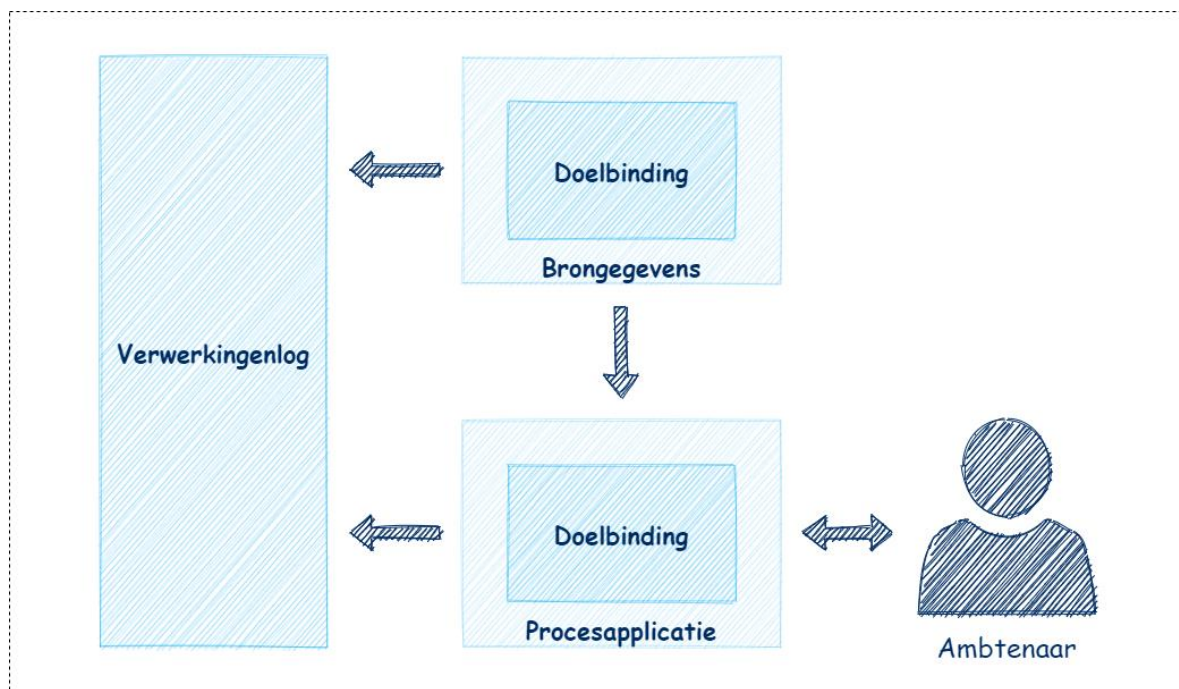
In bovengenoemd voorbeeld heeft de gemeente het Verwerkenlog via de MijnGemeente Pagina opengesteld. Als de burger de MijnGemeente Pagina niet kan gebruiken – bijvoorbeeld omdat burger geen computer tot zijn beschikking heeft – moet de burger de gegevens uit het Verwerkenlog via een medewerker van de gemeente opvragen. Ook kan een gemeente besloten hebben het Verwerkenlog niet via de MijnGemeente Pagina open te stellen, bijvoorbeeld omdat het Verwerkenlog te weinig betekenisvolle

gegevens voor de burger bevat. Ook in dat geval moet de burger via een medewerker van de gemeente de gegevens opvragen.

Het verzoek wordt door een bevoegde medewerker (bijvoorbeeld een Privacy Officer of Functionaris Gegevensbescherming) in opdracht van de burger uitgevoerd. Alleen de verwerkingsactiviteiten die betrekking hebben op de burger worden opgehaald. Omdat het VWL alleen de unieke nummers van de verwerkingsactiviteiten bevat, moeten de loggegevens gecombineerd worden met de gegevens uit het VAR om aan de burger een begrijpelijk en samenhangend resultaat te kunnen tonen. Het opvragen van de gegevens in opdracht van de burger wordt ook geregistreerd in het Verwerkingenlog omdat de persoonsgegevens van de burger zijn geraadpleegd.

6.2. Brongegevens raadplegen

Met de ontwikkelingen van het GEMMA Gegevenslandschap en Common Ground worden Brongegevens apart opgeslagen van Procesapplicaties. Door gegevens bij de bron te bevragen wordt voorkomen dat er onnodig wordt gekopieerd en kunnen meerdere Procesapplicaties gebruikmaken van dezelfde gegevens. Onderstaande schets geeft aan hoe een Procesapplicatie Brongegevens uit een ander register opvraagt.



Figuur 9 Brongegevens raadplegen

In het centraal Gemeentelijk register van verwerkingsactiviteiten zijn alle verwerkingsactiviteiten opgenomen die door de gemeente kunnen worden uitgevoerd. Een Procesapplicatie voert maar een aantal verwerkingsactiviteiten uit het gehele register uit. Het ligt daarom voor de hand dat elke Procesapplicatie alleen de UUID's van die verwerkingsactiviteiten uit het centrale register overneemt die van belang zijn. Elke

applicatiefunctie in de Procesapplicatie dat een persoonsgegevensverwerking uitvoert, wordt gekoppeld aan zo'n verwerkingsactiviteit en vastgelegd als Doelbinding in de Procesapplicatie. Dit gebeurt tijdens de configuratie of inrichting van een (nieuwe) Procesapplicatie of als er wijzigingen zijn doorgevoerd in het VAR die van belang zijn voor de Procesapplicatie.

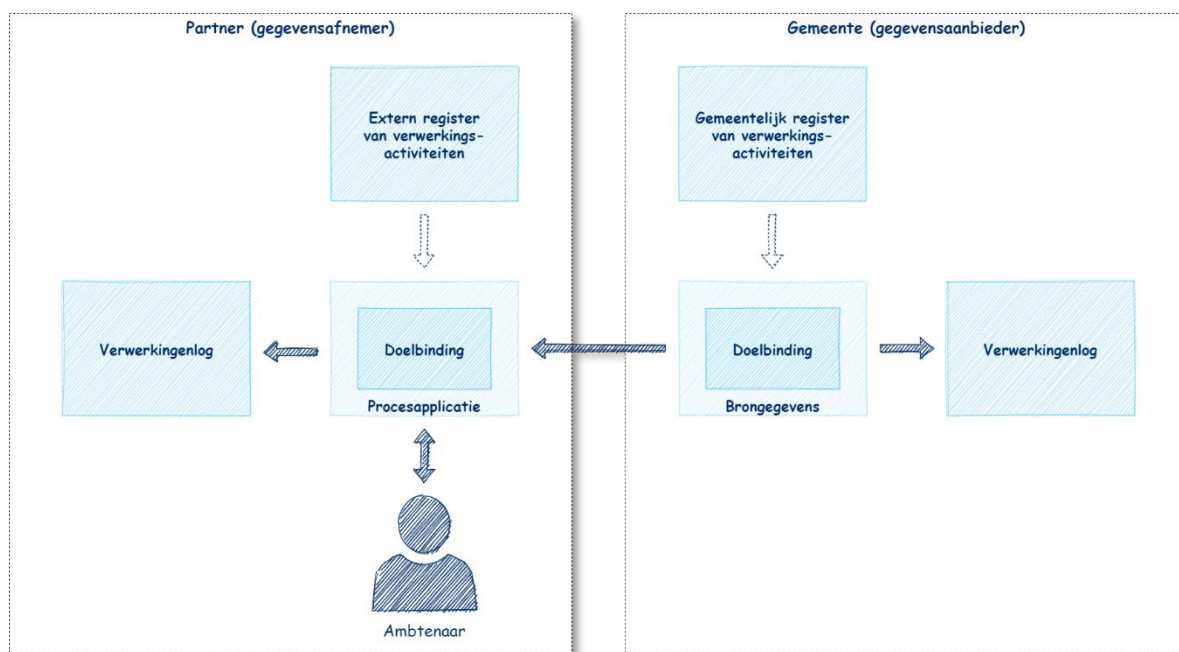
Dit geldt ook voor de Brongegevens. Elke functie in het register dat een persoonsgegevens-verwerking uitvoert wordt gekoppeld aan een verwerkingsactiviteit en vastgelegd als Doelbinding. Ook dit gebeurt alleen tijdens de configuratie of inrichting van een (nieuwe) register met Brongegevens of als er wijzigingen zijn doorgevoerd in het VAR die van belang zijn voor het register Brongegevens.

Als een Ambtenaar persoonsgegevens via een Procesapplicatie gaat verwerken, wordt de verwerkingsactiviteit die daarbij hoort eerst vastgelegd in het VWL. Daarna worden de Brongegevens bevraagd. Voordat de gegevens aan de Procesapplicatie worden verstrekt, wordt door het register Brongegevens eerst in het VWL vastgelegd welke verwerkingsactiviteit door het register Brongegevens worden verwerkt. Daarna worden de Brongegevens aan de Procesapplicatie verstrekt.

Zowel de Procesapplicatie als de Brongegevens gebruiken een eigen Doelbinding en beide leggen ook een eigen verwerkingsactiviteit vast in het VWL.

6.3. Gegevens aanbieden aan externen

Gemeenten beschikken over gegevens die door andere organisaties opgevraagd kunnen worden. Een gemeente kan dus aanbieder zijn van gegevens aan keten- en netwerkpartijen. Onderstaande schets geeft een globaal beeld hoe gegevensuitwisseling tussen een gemeente en keten- of netwerkpartij kan plaats vinden.



Figuur 10 Brongegevens aanbieden

Als een keten- of netwerkpartij gegevens bij een gemeente bevraagt, doet deze partij dat vanuit de eigen Procesapplicatie met een eigen doel en grondslag (verwerkingsactiviteit). In de Procesapplicatie is in de Doelbinding vastgelegd voor welke actie welke specifieke verwerkingsactiviteiten gebruikt worden. Deze verwerkingsactiviteiten zijn overgenomen (vaak alleen het unieke ID) uit het centraal Extern register van verwerkingsactiviteiten. De Procesapplicatie legt het unieke ID van deze verwerkingsactiviteit – bijvoorbeeld 'Raadplegen persoonsgegevens bij gemeente' – vast in het eigen Verwerkingenlog.

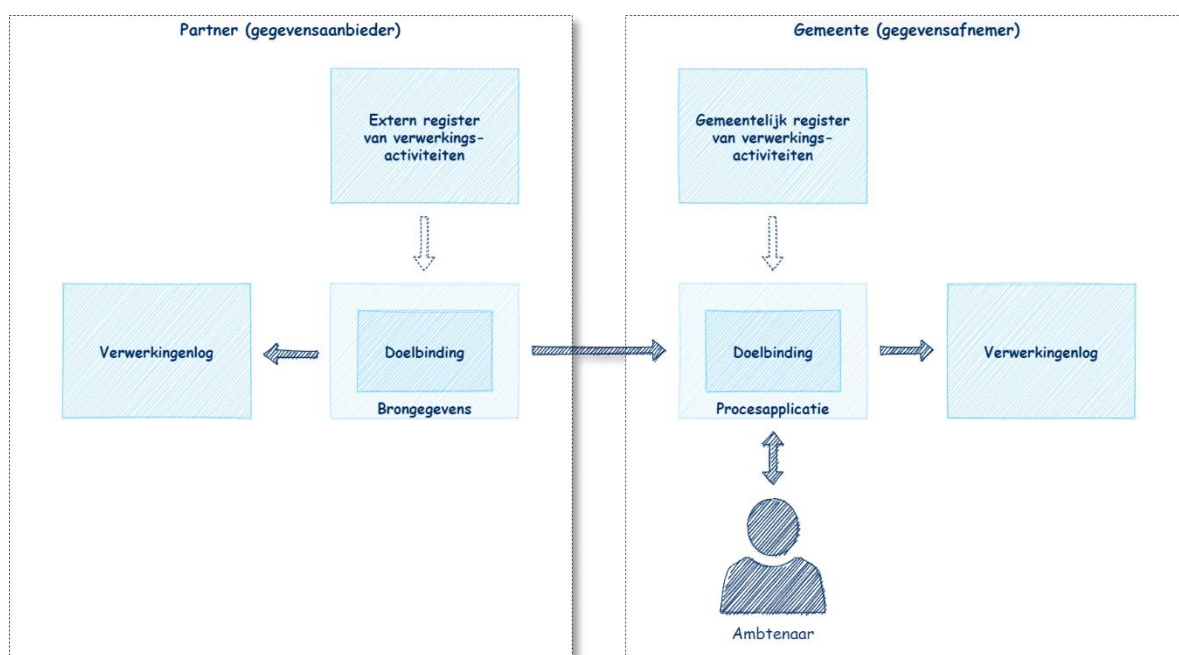
Daarna zal de verbinding naar de Brongegevens van de gemeente worden gelegd. Uiteraard heeft de gemeente een informatiesysteem om te controleren of de partner überhaupt wel gegevens bij de gemeente mag ophalen (authenticatie en autorisatie). Dit informatiesysteem is vanwege de leesbaarheid van de schets achterwege gelaten.

De component bij de Gemeente waarin de Brongegevens staan bevat in de Doelbinding ook een overzicht van unieke ID's die zijn overgenomen uit het centraal Gemeentelijk register van verwerkingsactiviteiten waarin staat dat de gegevens bevraagd worden in het kader van een verzoek van een ketenpartner – bijvoorbeeld 'Opvraging persoonsgegevens door ketenpartner'. Het unieke ID van de verwerkingsactiviteit wordt geregistreerd in het Verwerkingenlog van de Gemeente waarna de Brongegevens aan de ketenpartner worden geleverd.

Zowel de Procesapplicatie van de Partner als de Brongegevens bij de Gemeente gebruiken een eigen Doelbinding en beide organisaties leggen ook een eigen verwerkingsactiviteit vast in hun eigen VWL.

6.4. Gegevens afnemen bij externen

Andere organisaties beschikken over gegevens die door Gemeenten opgevraagd kunnen worden. Een Partner kan dus aanbieder zijn van gegevens aan een Gemeente. Onderstaande schets geeft een globaal beeld hoe gegevensuitwisseling tussen een gemeente en keten- of netwerkpartij kan plaats vinden.



Figuur 11 Brongegevens afnemen

Als een Gemeente gegevens bij een keten- of netwerkpartij bevroegt, doet de Gemeente dat vanuit de eigen Procesapplicatie met een eigen doel en grondslag (verwerkingsactiviteit). In de Procesapplicatie is in de Doelbinding vastgelegd voor welke actie welke specifieke verwerkingsactiviteiten gebruikt worden. Deze verwerkingsactiviteiten zijn overgenomen (vaak alleen het unieke ID) uit het centraal Gemeentelijk register van verwerkingsactiviteiten. De Procesapplicatie legt het unieke ID van deze verwerkingsactiviteit – bijvoorbeeld 'Raadplegen persoonsgegevens bij ketenpartner' – vast in het eigen Verwerkingenlog.

Daarna zal de verbinding naar de Brongegevens van de Partner worden gelegd. Uiteraard heeft de Partner een informatiesysteem om te controleren of de Gemeente überhaupt wel gegevens bij de ketenpartner mag ophalen (authenticatie en autorisatie). Dit informatiesysteem is vanwege de leesbaarheid van de schets achterwege gelaten.

De component bij de Partner waarin de Brongegevens staan bevat in de Doelbinding ook een overzicht van unieke ID's die zijn overgenomen uit het centraal Extern register van verwerkingsactiviteiten waarin staat dat

de gegevens bevestigd worden in het kader van een verzoek van een Gemeente – bijvoorbeeld ‘Opvraging gegevens door gemeenten’. Het unieke ID van de verwerkingsactiviteit wordt geregistreerd in het Verwerkingenlog van de Partner waarna de Brongegevens aan de Gemeente worden geleverd.

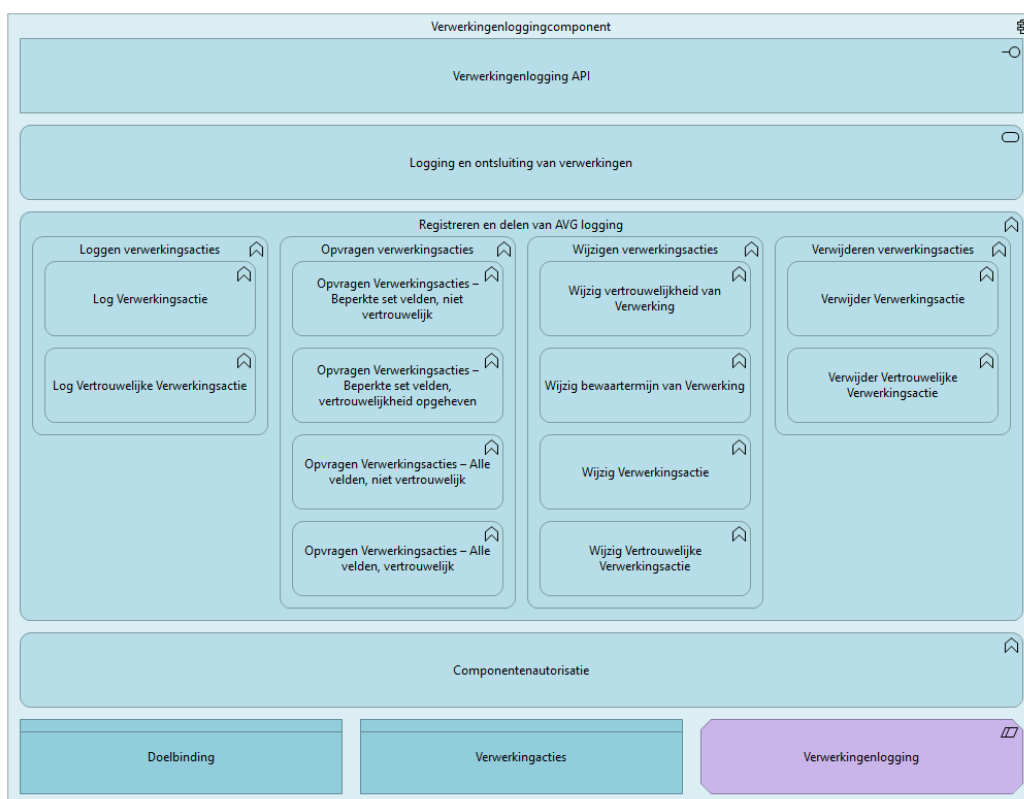
Zowel de Procesapplicatie van de Gemeente als de Brongegevens bij de Partner gebruiken een eigen Doelbinding en beide organisaties leggen ook een eigen verwerkingsactiviteit vast in hun eigen VWL.

7. GEMMA componenten

In de voorgaande hoofdstukken is beschreven dat gemeenten vanuit de AVG verplicht zijn om logging van verwerkingen bij te houden. Van de verwerkingen worden diverse metadata opgeslagen in een loggingregister. Onderdeel van de metadata zijn doelen en wettelijke grondslagen van. Het loggingregister wordt door VNG Realisatie breder gepositioneerd dan enkel voor de verwerkingen van persoonsgegevens. Dit register gaat ook verwerkingen van andere objecten bevatten.

7.1. Verwerkingenloggingcomponent

Het verwerkingenloggingcomponent wordt gebruikt voor opslag en ontsluiting van het verwerkingenlog. Het verwerkingenloggingcomponent ondersteunt de opslag van metagegevens die gerelateerd zijn aan een verwerking van gegevens conform het informatiemodel verwerkingenlogging. De logginggegevens worden door gemeentelijke informatiesystemen aan de verwerkingenloggingcomponent aangeleverd via de gestandaardiseerde Verwerkingenlogging API-standaard. Deze API-standaard biedt functies voor het zoeken in de logging en het bevragen van de logging.



Figuur 12 Onderdelen verwerkingenloggingcomponent

Een verdere uitleg van de verwerkingenloggingcomponent en enkele uitwerkingen van de verschillende interactiepatronen is te vinden op een aparte pagina op GEMMA Online (https://www.gemmaonline.nl/index.php/Interactiepatronen_Verwerkingenlogging).

Bijlage 1: Bronnen

- NL DIGIbeter 2020: Agenda Digitale Overheid, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 2020,
<https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2020/07/nl-digibeter-2020.pdf>
- Nederlandse digitaliseringsstrategie, Rijksoverheid.nl
<https://www.rijksoverheid.nl/documenten/rapporten/2020/06/25/nederlandse-digitaliseringsstrategie-2020>
- Onderzoeksrapport Waardevol digitaliseren, Rathenau Instituut, juni 2018
https://vng.nl/files/vng/rapport-rathenau_instituut_waardevol_digitaliseren.pdf
- Aanwijzing logging, Gemeentelijke Informatiebeveiligingsdienst, januari 2014
<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>
- Checklist Data Privacy Impact Analyse, Gemeentelijke Informatiebeveiligingsdienst, augustus 2018,
<https://www.informatiebeveiligingsdienst.nl/nieuws/checklist-data-privacy-impact-analyse/>